NOTE: The Albuquerque Operations Office (ALO) developed this study material in support of the Technical Qualification Program's Problem Analysis/Risk Assessment area. It is added to this study guide for your convenience. This study material supports Occupational Safety competency 1.2. This file is an exact copy of the materials designed by ALO.

Hazard Analysis

Section 5

OBJECTIVE

Demonstrate knowledge of hazard analysis techniques applicable to systems, processes/operations, and

1. Demonstrate knowledge of hazard analysis techniques applicable to systems, processes/operations, and jobs.

5 - 1

A. For a given operation, identify and perform appropriate job safety analysis techniques, and make necessary recommendations.

The definition of hazard evaluation as defined by the American Institute of Chemical Engineers (AICHE) is the following:

> The analysis of the significance of hazardous situations associated with a process or activity. This analysis uses qualitative techniques to pinpoint weaknesses in the design and operation of facilities that could lead to accidents.

The process of assessing project risks to identify critical systems, subsystems, and other factors requiring focused work and resolution is summarized by the questions:

- What could go wrong?
- How likely is it?
- What are the consequences?

How the process is applied consists essentially of the following:

- Establish the scope of the study. (The scope will include earthquakes, tornadoes, flooding, internal failures, sabotage, study boundaries, etc.)
- Identify the hazards.
- Identify the parts of the process or system that give rise to the hazards identified.
- Classify hazards into Category 1, 2, and 3 according to hazard consequences.

- Identify all active systems, barriers, components, and other passive design features designed to address or mitigate Category 1 and 2 (and in some cases Category 3) hazards.
- Prepare and document a Preliminary Hazards Analysis (PHA) to further qualify accident sequences (Optional). Another equivalent technique may be used.

Generally, for a hazard evaluation, qualitative and lesser quantitative techniques are used to arrive at a hazard determination as defined by the following hazard category levels:

- Category 1: Hazards show significant offsite consequences
- Category 2: Hazards show significant onsite consequences
- Category 3: Hazards show only localized consequences.

The end result of the hazard evaluation without a PHA is the identification of those hazards that have adverse impacts on the population or the environment as well as adverse economic impacts such as a negative image or loss of market share. The PHA takes the process one step further and identifies structures, systems, components, administrative controls, and any other factors that are required to maintain qualitatively acceptable risk levels.

There are various hazard evaluation techniques which may be employed to identify and define hazards and in some cases further identify an accident sequence. The following is a list of techniques which may be used for hazard analysis:

- Preliminary Hazards Analysis (PHA)
- Failure Modes and Effects Analysis (FMEA)
- Failure Modes and Effects Criticality Analysis (FMECA)
- Hazard and Operability Analysis (HAZOP)
- Event Tree Analysis (FTA)
- Fault Tree Analysis (ETA)
- Energy Trace and Barrier Analysis
- Operating and Support Hazard Analysis
- System/subsystem Hazard Analysis
- Hazard Evaluation
- Human Reliability Analysis (HRA).

The more commonly used techniques are discussed in further detail under Objective 1.B. All techniques seek to identify the hazards that

could be a source of risk. Some techniques further classify the hazards, and still others further define accident mitigation or prevention functions. Examples of hazards are the following:

- Combustible Material
- High Pressure Piping
- Caustic/Corrosive Chemicals
- Chemical Solutions
- Radionuclide Inventory
- Potential Energy (e.g. Dams, Objects suspended at high height, etc.)
- Biological Hazards
- Toxic Hazards
- Kinetic Energy (e.g. Rotating Machinery, Rivers, etc.)
- Electrical Energy
- High Temperatures
- Cryogenics.

Ultimately, based upon a hazard analysis of a facility or process, hazards are identified which have unacceptable risk. From this analysis and from further analysis, mitigating or preventive measures may be identified to address the risk. As a result, recommendations may be made and incorporated into design or subsequent facility modifications to reduce risk to acceptable levels and within acceptable costs.

It is important to understand that the hazard evaluation process (at best) generally provides a relative, non-absolute evaluation or ranking of risk issues. In fact, some techniques may provide not ranking information at all. This in part is one reason for the necessity of continuous reevaluation throughout facility life cycle as issues and new hazards or accident types are introduced, discovered, or existing ones become better defined or understood.

B. Discuss the need for, and the selection and performance of the applicable qualitative techniques of system safety analysis, such as:

- **Preliminary Hazard Analysis (PHA)**
- **Failure Modes and Effects Analysis (FMEA)**
- **Failure Modes and Effects Criticality Analysis (FMECA)**
- **Fault Tree Analysis (FTA)**
- **Event Tree Analysis (ETA)**
- **Fault/Event Tree Analysis**
- **Hazard and Operability Analysis (HAZOP)**
- **Energy Trace and Barrier Analysis**
- **Human Reliability Analysis (HRA)**
- **Operating and Support Hazard Analysis**
- **Hazard Evaluation**

Preliminary Hazard Analysis (PHA)

PHA techniques are frequently used when it is desired to include the analysis of event sequences that transform hazards into accidents. Additionally, PHA considers corrective measures and consequences of an accident. Table 5.1 represents the preliminary hazard analysis format for two hazardous situations:

1. hydrochloric acid is introduced into water
2. high temperature chloride-water mixture introduced into stainless steel tank.

Table 5.1

Preliminary Hazard Analysis Example Format

Hazardous Element	Exothermic Reaction	Corrosion/Pitting
Triggering Event 1	Hydrochloric acid introduced into water	Contents of stainless steel tank contaminated with high temperature chloride-water mixture
Hazardous Condition	Potential to initiate strong acid ionization reaction	Chloride pitting inside stainless steel tank
Triggering Event 2	Container outside of hood	Operating pressure of tank exceeded
Potential Accident	Explosion, acid dispersal/splash	Stainless steel tank rupture
Effect	Personnel injury and acid burns; Damage to surrounding structures	Personnel injury from explosive energy and burns; Damage to surrounding structures
Corrective Measures	Add water into hydrochloric acid; disseminate lessons learned on above hazards; perform reactive chemistry inside hoods; wear personal protective equipment (PPE)	Use mild steel or a lined tank; eliminate chlorides; locate tank at a suitable distance from personnel and equipment

Figure 5.1 has been adapted from “Guidelines for Hazard Evaluation Procedures,” (see References), and summarizes the process of hazard identification, hazard evaluation, and risk analysis. Figure 5.1 is located at the end of this section on page 5-13.

In general, PHAs attempt to identify the system events and hardware that can lead to hazards. This step is normally performed during the initial design phase so that insights may be incorporated into designs.

Failure Modes and Effects Analysis (FMEA)

The FMEA process is an inductive logic approach to the identification of all possible failure modes and their effects for all equipment on a component-by-component basis. This process identifies single failure modes only in accordance with the requirements of IEEE 279-1971, 10 CFR Appendix K, and Regulatory Guide 1.7. A FMEA is generally

much more detailed than a fault tree analysis since all failure modes are considered rather than only considering dominant ones as is typical in a fault tree analysis. As an example, the failure modes for a relay are presented in Table 5.2.

Table 5.2

Sample Relay Failure Modes

◆ contacts stuck open
◆ contacts stuck closed
◆ contacts slow to open
◆ contacts slow to close
◆ contacts bent, no contact
◆ contact short circuit
  ◦ to ground
  ◦ to supply
  ◦ between contacts
  ◦ to signal lines
◆ contacts arcing, generating noise
◆ contacts oxidized, current low
	◆ contact resistance
	  ◦ high
	  ◦ low
	◆ coil overheating/breakdown
	◆ coil open circuit
	◆ coil short circuit
	  ◦ to supply
	  ◦ to contacts
	  ◦ to itself
	◆ contact - coil armature arm mechanically stuck
	◆ relay overmagnetized or excessive hysterisis

As a consequence of the analysis, a qualitative, systematic list of equipment, failure modes and associated effects is developed. The worst case consequences of a single failure are also given with recommendations for improving safety for individual failures. The end result is the generation of recommendations for increasing equipment reliability and thus improving safety.

Failure Modes and Effects Criticality Analysis (FMECA)

The use of the word “criticality” in this technique refers to the assignment of a severity attribute to a component failure in an FMEA. This technique may be used within a FMEA or another analysis to extend the analysis and include or rank failure severity. Hence, where this method is employed in FMEA as well as other hazard evaluation techniques, it merely attempts to assign a severity attribute to an individual or conservatively to a similar group of failures in the interest of bounding risk. This process may be used to scope hazard severity and assist in the prioritization of hazards and accidents.

Fault Tree Analysis (FTA)

The FTA process is a deductive technique used to identify combinations of equipment failures, other structures or phenomenological events, or external event failures that can result in the transformation of a hazard into an event of concern or an accident. The results are quantitative in nature which allows relative risk ranking for individual or combinations of failures that may lead to the event of concern and generally unacceptable risk. This technique was addressed in Section 2.

Event Tree Analysis (ETA)

An event tree analysis considers the responses of safety systems, operators, and any related phenomenological events to an initiating event and determines the various possible outcomes from the accident. The results of an event tree analysis are sequences of events defined by successes or failures of individual events leading to accident sequences. Event tree analysis is best suited for analysis of complex facilities where there are multiple preventive or mitigative barriers along with systems or emergency procedures designed to respond to specific initiating events. The structure of event trees was addressed in Section 2.

Fault/Event Tree Analysis

A fault tree/event tree analysis is generally performed to develop a more detailed, quantified picture of facility or integrated systems risk where there are likely to be a number of support systems whose failure could collectively impact mitigative or preventive structures, systems, components, or barriers. The process involves development of event trees that model accident progression for all sequences of interest. This is accomplished by creating an event tree for a single or a group of similar hazards/accidents where the response of preventive or mitigative SSCs would be expected to be the same. For each event tree top requiring more than just a simple yes/no quantification, a fault tree is usually developed that includes interdependencies between SSCs and:

- the initiating hazard or event
- other event tree top SSCs
- the accident progression environment.

An example of the first dependency would be the loss of a common (normal) cooling water supply to a normal cooling water system where the water supply is also the normal supply for another separate core injection system. In this instance, if the water supply were to be lost or became non-functional, the loss of normal cooling water would act as an initiator while the loss of the core injection system would simultaneously be defeated. For the second dependency, if the system fails to provide power, all subsequent system components requiring electric power downstream from the failure could be non-functional. This example may be limited to failure of equipment fed from a common breaker, panel, etc., or it could be as involved as a site/facility blackout depending on the cause of the initial loss, i.e., it could be a failed breaker, a bus, a transformer, or loss of off-site power. For the third example, an internal flooding incident where a pipe break from a cooling system could spray or flood out surrounding equipment and result in their inability to perform as designed.

Upon completion of the development of all fault trees, the sequences are written in terms of a Boolean equation that combines the combinations of successes and failures to represent a single event tree sequence. When this is completed for all sequences of all accident types, the resulting sequences are solved using a computer; and numerical results representing minimal cut set failures are calculated. A running total of all unique cut sets is calculated to determine the total combined sequence risk frequency. Further studies may be performed on the results to determine individual (fractional) sequence, system, component, etc. contribution to risk.

Hazard and Operability Analysis (HAZOP)

This technique was developed to identify and evaluate safety hazards in a process plant and to identify operability problems which, although not necessarily hazardous, may result in the inability of a plant or process to achieve design productivity. To perform a HAZOP analysis, original and current (if modified) design and operating information must be available. Consequently, HAZOP analyses are most commonly performed immediately following the detailed design phase. Similar to the PHA, an interdisciplinary team uses a creative, systematic approach that identifies hazard and operability problems that may result from deviations in process design intent.

The purpose of the HAZOP analysis is to systematically review a process or operation to determine whether process deviations can lead to undesirable consequences. The process may be used for either batch or continuous processes as well as for evaluation of written procedures. A simple example of a batch process would be the titration of one substance into a mixing container while for a continuous process, the oil cracking process, would contain several such examples. Where the team discovers that there is inadequate protection against a given process deviation, a recommendation is made to reduce risk.

Using the HAZOP process, the team is likely to:

- identify both hazards and operating problems
- make recommendations for design, administrative, or procedural changes that may improve the system as well as recommendations for further study.

Energy Trace and Barrier Analysis

The energy trace and barrier analysis method is a systematic process used to identify physical, administrative, and procedural barriers or controls that should have prevented the occurrence. This technique should be used to determine why these barriers or controls failed and what is needed to prevent recurrence. A sample Barrier Analysis is found in Section 4.

Human Reliability Analysis (HRA)

Human Reliability Analysis is the systematic process of evaluation of human performance and associated impacts on SSCs for a facility. The process is generally applied to analyze the factors that influence the performance of operators, supervisors, maintenance personnel, and any other personnel that may influence accident sequence progression and severity. HRA techniques are generally used to analyze errors of omission such as failure to follow a specified procedure rather than errors of commission which are difficult to predict and/or may actually be outright acts of sabotage. The process identifies potential human errors and their effects including underlying causes if possible.

HRA is generally an input into other types of analysis such as fault tree/event tree. It is used to quantify specified human performance such as the use of a procedure that directs the operator/supervisor to

initiate emergency core cooling upon initiation of a large loss of cooling accident. It may also be used to perform isolated analysis of individual operating or maintenance procedures in order to better understand the larger contributors to the risk associated with performance of a specified operation or procedure. The process lists the errors likely to be encountered during performance of a given procedure, factors influencing performance, and those proposed modifications likely to reduce errors during performance. The analysis also identifies those system interfaces that are affected by such errors.

Operating and Support Hazard Analysis

This process is a subset of the hazard evaluation process discussed in the next paragraph.

Hazard Evaluation (including system and subsystem)

The hazard evaluation process has been performed by the chemical process industry in excess of 35 years. Historically, the process has been known by several different names including process hazard analysis, process hazard review, process safety review, process risk review, predictive hazard evaluation, hazard assessment, process risk survey, and hazard study.

To perform a hazard evaluation, all hazards associated with a facility or process to be studied must first be identified. Upon completion of this phase, the hazard evaluation process focuses on the potential causes and consequences associated with those hazards that are created from episodic or catastrophic events.

An example would be an accidental release of gas from a storage cylinder. This is opposed to those hazards that routinely exist at a facility or may occasionally occur. An example of these would be slips from ladders, injury from the use of industrial tools such as drills or saws, continuous releases of exhaust gases from internal combustion engines, or intentional process exhaust from a stack.

The latter hazards are normally addressed by design considerations and good housekeeping practices. Hazard evaluation however attempts to focus on the facility internal SSC failures, external events, and human influenced performance events that may lead to catastrophic releases of energy, toxic, radiological, and biologically harmful materials that may harm the surrounding environment.

Summary

Hazard evaluations normally involve the combined efforts of a multi-disciplinary team that combines the experience, judgment, and expertise to address the diverse range of problems and recommend solutions or further studies. Where information is inadequate and further study is warranted, techniques involving more quantitative risk assessment measures are often employed to give the team additional information needed for decision making. For further assistance in the use of the hazard evaluations process, the student is to refer to the worked examples in the Second Edition of Hazard Evaluation Procedures.

C. Describe the bases upon which to judge the adequacy of a hazard evaluation.

The bases for judging adequacy of a hazard evaluation includes the consideration of a number of factors. These factors are discussed individually in the following subsections and typically consist of:

Thoroughness of hazard identification

The thoroughness of any hazard identification process is rooted in a systematic approach to the identification of all potential site/facility hazards. Typically this process involves two key tasks; identification of specific undesirable consequences, and, identification of material, system, process, and plant characteristics that could produce those consequences.

Identification of undesirable consequences typically consists of addressing such categories as physical impacts to humans or the environment and economic impacts including mitigative and recovery costs associated with the physical impacts. Once the undesirable consequences are identified, the analyst may begin to identify the systems, processes, and hazards of interest that warrant further investigation. Commensurate with this approach, grading of hazards in the form of a conservative screening analysis is also important so as to allow the analyst to focus on the most significant hazards for further evaluation.

Common methods for initial identification of hazards include analyzing process/facility material properties and conditions,

reviewing analyses for other similar facilities, reviewing industry process experience, developing interaction matrices, and applying hazard evaluation techniques. The latter process often identifies additional hazards through methodical analysis and comparison of accident initiation, progression, and mitigation. For additional detail on application of these and other techniques, the student is referred to Chapter 3 of **Guidelines for Hazard Evaluation Techniques** by the American Institute of Chemical Engineers.

Rigor of analysis versus complexity of operation and potential consequences of accidents

The more complex the system or operation, the more potential for an undiscovered or missed interaction or sequence of events that could lead to a hazardous condition. As a corollary, if the accident consequences are unacceptably high for accidents identified during the analysis phase, a more thorough analysis may also be necessary to demonstrate acceptable risk. This would imply that a more thorough analysis would be required for complex, multiple system facilities or for facilities where accident consequences have the potential to be unacceptable high.

Conservative assumptions and documentation of assumptions

In order to have credibility, any analysis performed must make conservative assumptions where data found does not support modeling and analysis. Additionally, any and all assumptions must be documented in order to permit duplication and validation of results. If assumptions are made and are not documented, any validation of results through a peer review process becomes difficult if not impossible. Further, if conservative assumptions are not made, any results are compromised in terms of demonstrating acceptable risk. This is the mathematical equivalent of multiplying multiple factors, all but one of which are conservative. As a result, the answer is not conservative, in fact, the position on the spectrum is unknown. If this process is repeated with results of numerous individual series of calculations (cutsets) summed, the results of the sum are inconclusive since each individual calculated series is indeterminate. Stated another way, the sum if indeterminate cutsets results in an indeterminate summation.

Applicability of data

Where data are analyzed for input into an analysis, results are more credible if plant or facility specific data are available and analyzed. In the absence of plant or facility specific data, data from an identical or similar facility is next best, followed by data from site or facility installed equipment manufacturers, and finally, generic data from other facilities with similar missions and equipment but not necessarily similar processes. Often times generic data may only be available for use in analysis, but when used, careful consideration should be given to incorporating data from similar equipment of component designs. There are numerous public and private domain databases that have been specifically developed to support risk based quantitative analyses. Examples include IEEE-500 and the Savannah River historic equipment reliability database.

Consistency and control of any expert elicitation process (if used)

In order to maintain credibility in the data analysis phase of an assessment where either historic data are not available, or where the data are determined to be inappropriate for use, an expert panel is normally established and specific questions are asked in order to determine a best estimate point value and uncertainty (probability distribution) factor. This process must be documented and follow defined guidelines which generally involve elicitation of experienced analysts, operators and operations management/supervision, and engineering personnel to determine failure probabilities or other necessary data in order to support a thorough analysis. Credibility and accuracy of results are supported through consistency of process application and credibility of the expert panel and the ensuing data analysis and determination.

Validity and conservatism of scenario screening criteria

In the performance of detailed analyses, there are normally tens to hundreds of accident scenarios that may need to be analyzed. Upon identification of all credible initiators and accident scenarios, an initial screening is normally performed. This initial screening allows the analyst to focus on those accident scenarios which need to be modeled in detail for further study. This process must document the screening criteria and must always fail to a conservative approach when performing a scoping analysis of individual scenarios. Documenting the basis including any assumptions and the screening process allows the results to be duplicated thus establishing the validity of the initial accident screening process.

Reflection of lack of knowledge in uncertainty estimates
Uncertainty in data distributions is normally reflected in terms of an uncertainty estimate. Where data analysis indicates a wide distribution of (failure) data values, it is important to reflect this in the uncertainty (distribution) of data through the use of realistic or conservative uncertainty estimates. In probabilistic based analyses, uncertainty is normally given in terms of an error factor.

D. Review existing hazard analyses and assess the applicability methodology and recommendations/ conclusions resulting from the analysis.

As part of an exercise for this section, access an existing hazard analysis from the local DOE Field Office. Review the document and assess methodology, recommendations, and conclusions for applicability. Discuss results with your supervisor.

E. Discuss the applicability and pu rpose of nuclear and non-nuclear hazard analysis techniques required during the life cycle of a DOE facility.

As discussed in the various methods under Sub-section 1.B, the various hazard analysis techniques may typically lend themselves to more efficient application at various times during the facility life cycle. The analyst generally will determine which technique to use to analyze hazards/risks according to four primary variables:

1. cost
2. scope – including the scope of hazards as well as those initiators to be analyzed
3. complexity of the facility, structure, system or component
4. public or political interest.

These factors may often be interrelated and may require analyses and iteration in themselves to arrive at an acceptable method that will satisfy/address all issues. Table 5.3, on the following page, is a summary of prioritization attributes of the more common Hazard Evaluation techniques.

F. Discuss the benefits of applying hazard analysis techniques during the design phase of a facility, operation process or piece of equipment.

The process of applying hazard analysis techniques during the design phase of a facility, operation process, or component allows for either a qualitative or quantitative assessment of design criteria against desired performance attributes. The identification of sub-standard performance attributes appears in the form of excessive risk thus allowing for design modification prior to facility, operation process, or component construction. The hazard analysis process is generally iterative and may be repeated several times prior to design finalization. It seeks to modify design details to achieve desired safety objectives and thereby reduce risk and associated costs prior to construction and operation.

Table 5.3

Prioritization of Hazard Analysis Techniques

Technique	Provides Accident Scenario Information	Provides Frequency Information	Provides Consequence Information	Event Ranking Possible	Comments
PHA	May	No	Yes	Crude hazard category ranking	Usually ranked by hazard categories: Negligible; Marginal; Critical; or Catastrophic
HAZOP Analysis	Usually	May	Yes	Crude consequence ranking	Analysis performed by a team of individuals. Uses interaction and brainstorming techniques
FMEA	Usually	No	Yes	Crude qualitative consequence ranking; for quantitative see FMECA	FMEA generally qualitative; for quantitative priority ranking of failure severity see FMECA
FMECA	Yes	Yes	Yes	Priority ranking of failure severity	The criticality assessment in a FMECA provides a simple quantitative risk ranking
FTA	Usually	Yes, based on size and number of cut sets and type of failures involved	No	Frequency ranking based on analysis and comparison of multiple fault tree events	Quantitative FTA techniques are available to estimate top event frequencies
ETA	Yes	Yes, based on number of accident scenarios and number and type of failures involved	Yes, consequence categories are assigned for each scenario	Yes (Gross, unless combined with a more thorough top event analysis technique)	Quantitative ETA techniques are available to estimate top event and sequence frequencies. Example: ETA/FTA/HRA combined analysis
HRA	Yes	Yes, based on number and length of scenarios and type of human errors involved	No	Frequency Ranking	Quantitative HRA techniques are available to estimate human error probabilities. Often used in support of other analysis techniques

G. Discuss the importance of change control and its impact on the identification and timing of appropriate hazard analysis.

Change control is the continuous process of documenting as-designed/as-built facility equipment configuration and administrative and procedural changes. During the various stages of a facility life cycle, control over facility configuration documentation must be maintained since it forms the basis for and the validity of any hazard evaluation or risk assessment. Upon the completion of a hazard evaluation or risk assessment, issues are often identified which may require facility modernization or updates, redesign or re-engineering, deletion or addition of SSCs, or administrative or procedural modifications. As these issues are identified, existing design or as-built documentation must be modified to reflect a change in design or actual facility changes. Therefore, the process of hazard evaluation or risk assessment is used during all phases of a facility life cycle in an iterative sense. The hazard/risk evaluation process seeks to identify safety issues before they become a problem. Consequently, its use must be continuous, forming an integral part of the life cycle management process for a facility**.**

References and Suggested Reading

References and Suggested Reading

Henley, E. J. and Kumamoto, H., Probabilistic Risk Assessment, The Institute of Electrical and Electronics Engineers, New York, NY, 1992.

Guidelines for Hazard Evaluation Procedures, Center for Chemical Process Safety, American Institute for Chemical Engineers, New York, NY, 1992

Tukey, J. W., Exploratory Data Analysis, Addison-Wesley Publishing Co., Reading, MA, 1977.